NETWORK BASED INTRUSION DETECTION USING DEEP LEARNING METHODS

A

RESEARCH PROPOSAL

SUBMITTED

IN PARTIAL FULFILLMENT TO THE REQUIREMENT

FOR

DOCTOR OF PHILOSOPHY

IN

FACULTY OF SCIENCES

DISCIPLINE COMPUTER APPLICATION

By

GEETA KOCHER

(Enrollment No. – 17404 FPE02)

Under supervision of

DR. GULSHAN KUMAR

MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY

BATHINDA (INDIA)

(March, 2019)

CONTENTS

Title	Page No.
Abbreviations	3
List of Tables	4
List of Figures	5
1. Introduction 1.1 Intrusion Detection System 1.2 Classification of IDS 1.3 Benchmark Intrusion Detection Datasets 1.4 Anomaly-based Intrusion Detection Techniques	6-12
2. Literature Review 2.1 Shallow Machine Learning Techniques for Intrusion Detection 2.2 Deep Learning Techniques 2.2.1Supervised Deep Learning Techniques 2.2.2 Unsupervised Deep Learning Techniques 2.3 Deep Learning Techniques for Intrusion Detection	12-23
3. Research Issues / Gaps	24-25
4. Problem Formulation	25
5. Research Objectives	25-26
6. Expected Contributions	26
7. Methodology	27
8. Place of Work	27
9. Resources (Hardware/Software/) required	27
10. Proposed Work Plan	28
Bibliography	29-33

ABBREVIATIONS

AE	Auto Encoder
AI	Artificial Intelligence
ANN	Artificial Neural Network
ANIDS	Anomaly-based Network Intrusion Detection System
BN	Bayesian Network
BM	Boltzmann Machine
CNN	Convolutional Neural Network
DAE	Deep Auto Encoder
DARPA	Defense Advanced Research Projects Agency
DBM	Deep Boltzmann Machine
DBN	Deep Belief Network
DL	Deep Learning
DNN	Deep Neural Network
DR	Detection Rate
FN	False Negative
FP	False Positive
FPR	False Positive Rate
FNR	False Negative Rate
GPU	Graphical Processing Unit
HIDS	Host-based Intrusion Detection System
IDS	Intrusion Detection System
KDD	Knowledge Discovery Dataset
LSTM	Long Short Term Memory
ML	Machine Learning
NIDS	Network-based Intrusion Detection System
NN	Neural Network
PSO-FLN	Particle Swarm Optimization-Fast Learning Network
RBM	Restricted Boltzmann Machine
RNN	Recurrent Neural Network
SAE	Stacked Auto Encoder
SVM	Support Vector Machine

LIST OF TABLES

TABLE 1 Description of Available Benchmark Datasets

TABLE 2 A literature review of shallow machine learning techniques

TABLE 3 Summarized Review of Deep Learning Techniques for NIDS

LIST OF FIGURES

FIGURE 1	Targeted attacks in Top 10 Countries between 2015 and 2017
FIGURE 2	Classification of IDS
FIGURE 3	Categorization of Anomaly Techniques
FIGURE 4	Architecture of CNN
FIGURE 5	Architecture of AE
FIGURE 6	Architecture of RNN
FIGURE 7	Architecture of Boltzmann Machine
FIGURE 8	The Proposed Methodology

1. Introduction

With the growth of the Internet and its potential, more and more people are getting connected to the Internet. It is expected that 50 billion devices will be connected to the internet in 2020 [1,3]. Although these facilities provide a lot of benefits to society and changed the world, but also brings a lot of security risks to the business over the network. Fig. 1 depicts targeted attack information in top 10 Countries between 2015 and 2017 [2].

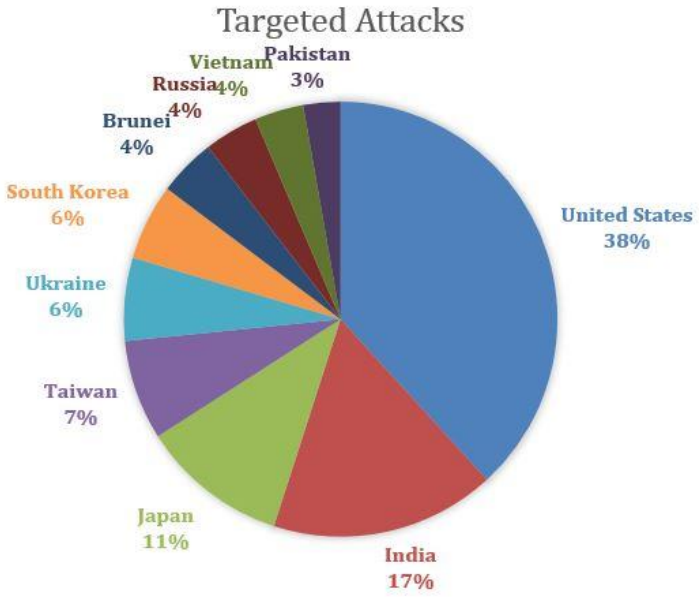

Figure 1: Targeted attacks in Top 10 Countries between 2015 and 2017

By taking the increasing number of attacks into consideration, network security has become a main issue at the present time. There should be some mechanism in the organizations to secure the data by maintaining the confidentiality, integrity and availability of data.

Currently, intrusion detection systems (IDS) provide an effective security solution in addition to traditional security methods like firewall, encryption and antivirus software for the network security. These traditional packages provided the first level of defence and failed to fully protect the networks and systems from increasingly attacks and malware. IDS acts as an additional security technique for securing computers and networks. IDS can be deployed on Host and Network. Host-based IDS (HIDS) resides on a host only and checks the intrusions on a particular host [47]. The drawback of HIDS is that it requires separate IDS for every host. For overcoming the limitations, IDS can be deployed on Network known as Network based IDS (NIDS). NIDS are independent of the operating system and extremely portable [49]. It protects hundreds of computers within a single network, which makes it

cheaper. So at the present time, there is a requirement to deploy the IDS on the network rather than Host to reduce the cost.

NIDS can use Signature or Anomaly methods to detect intrusions. Signature-based NIDS (SNIDS) work on prior prepared patterns of known attacks also called signatures. The benefit of SNIDS is a high accuracy to find known intrusions with low false alarm rates but criticized for incapability to detect novel attacks. It requires regularly update the database which is not feasible and a costly process [46]. Anomaly-based NIDS (ANIDS) deals with profiling user behaviour. In this approach, a certain model of user normal activity is defined, and any deviation from this model is known as anomalous [46]. The benefit of ANIDS is to predict the novel attacks. Due to several advantages of anomaly detection, we will focus on ANIDS in this research.

The anomaly-based IDS techniques are further classified as Statistical, Knowledge-based and Machine learning techniques [45]. Keeping the advantages of machine learning techniques like resilience to noisy data, robustness, and adaptability into considerations, most of the researchers work on these techniques. These techniques have shown excellence in terms of low false alarm rate and high detection rate in comparison to Statistical and Knowledge-based techniques [60]. However, machine learning techniques suffer from the limitation of Manual feature extraction, inefficient to handle large amount as well as a variety of data, unable to detect multi-classification attacks [32].

In real-world applications, it is found that deep learning techniques can further improve accuracy by reducing the false alarm rate and increasing the detection rate [52]. Although it is a branch of machine learning, it is a broader version of machine learning in terms of complexity of structure and learning data representations. Fortunately, deep learning techniques are known for their abilities to handle labelled or unlabeled data and solve complex problems with the help of the high powered GPU, reduces the need of feature engineering which is the most time-consuming part of machine learning [50]. Deep learning techniques provide accurate information since they can pinpoint the main problem. The system depends upon the data patterns to detect the problem which would be difficult to observe with human analysts. Deep learning techniques have been successfully applied in the area of natural language processing, speech recognition, computer vision, audio recognition, machine translation and social network filtering [41].

A large number of deep learning techniques have been proposed in the literature. The significant deep learning techniques include Auto Encoder (AE) [16-23,38], Convolutional

Neural Network (CNN) [15], Deep Neural Network (DNN) [34-36], Boltzmann Machine (BM) [48], Recurrent Neural Network (RNN) [24-33] and their variants like a Restricted Boltzmann Machine (RBM) [37,39], and Deep Belief Network (DBF) [40,48] as depicted in the Figure3. Currently, these techniques are being used in the field of image processing, computer vision. But, a few researchers have applied Deep Learning Techniques for detecting the network intrusions[34]. In this work, we focus on the employment of deep learning techniques for effective detection of network intrusions.

1.2 Intrusion Detection Systems

IDS can be a device or software system that monitors the network for detecting malicious activity. The attacks bypassed by the firewall are detected by IDS. It continuously monitors the network, finds vulnerable parts of the network and informs the administrator about intrusions [51]. IDS has different tasks for performing the analysis of network traffic like data collection, pre-processing of data, intrusion recognition, reporting the administrator, and response [51].

1.3 Classification of IDS:

IDS can be classified on the basis of the method used for detection of intrusions, the reaction of IDS to a detected intrusion or data collection as depicted in Figure 2.

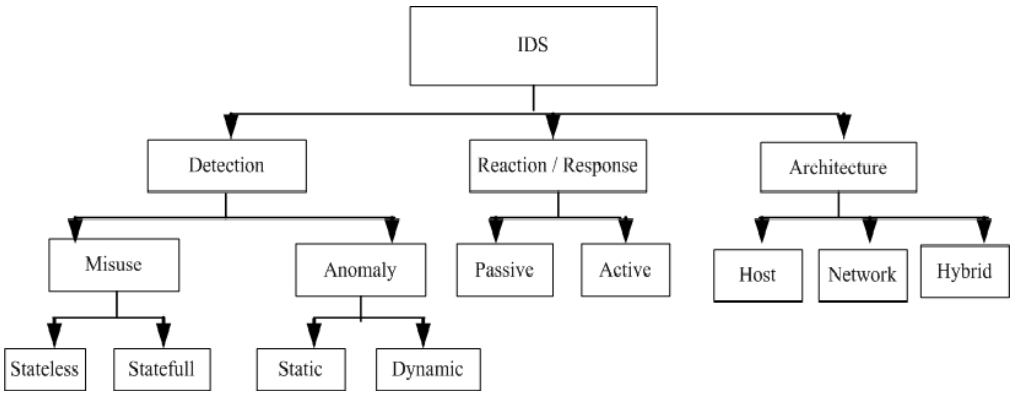

Figure 2: Classification of IDS

Detection methods of IDSs:

IDSs can be divided into two categories on the basis of the method used for detecting intrusions: Misuse Detection and Anomaly Detection. Misuse Detection operates with prior prepared patterns of known attacks also called signatures [43]. Stateless misuse detection systems use only existing signature whereas Stateful misuse detection systems use not only existing signatures, but also previous signatures. The approach has been used widely because of high accuracy to find known intrusions with low false alarm rates but criticized for

incapability to detect novel attacks [44]. One of the solutions to address this problem is to regularly update the database which is not feasible and a costly process. So, anomaly detection techniques came into existence. Anomaly Detection deals with profiling user behaviour [53]. In this approach, a certain model of user normal activity is defined, and any deviation from this model is known as anomalous. Anomaly detection methods are further categorized into two parts: Static anomaly detection and Dynamic anomaly detection. Static anomaly detection works on a principle that only a fixed part of the system which does not change is monitored like operating system software whereas dynamic anomaly detection extracts patterns (sometimes called profiles) from network usage history. It sets a threshold to separate normal consumption from anomalous consumption of resources. This method can detect novel attacks, but may lead to a high rate of false alarm rate and lacks high accuracy [56]. Another drawback is, if an attacker knows that he/she is being profiled, they can slowly change the profile to train the anomaly detection system of intruder's malicious behaviour as normal [56].

Reaction Methods of IDSs:

IDSs can be categorized as passive or active. Passive IDS only inform the administrator about the intrusion by generating alarms whereas Active IDS, not only inform the administrator about intrusion but also takes action by blocking the operation.

The architecture of IDSs:

IDSs can be installed on the host, on the network or on both (host and network), i.e. hybrid. The term "host" refers to an individual computer. Thus, each machine requires a separate sensor. This approach extracts a cost in performance, which might be unacceptable for customers running computationally greedy applications. Network-based IDS offer a different approach. Network-based systems are extremely portable. They are independent of the operating systems and only monitor traffic over a specific network segment. Deployed network-based intrusion detection sensors will listen for all attacks, regardless of the destination operating system type. The network-based solutions are easier to implement, but they can not keep up with heavy traffic or high volume speed. A system that integrates both host and network-based characteristics seemed the most logical approach intuitively and known as the Hybrid approach.

1.3 Benchmark Intrusion Detection Datasets

This section presents the detail of benchmark datasets that are available in the field of NIDS. Table 1 contains a description of available benchmark datasets. Most of the available datasets are imbalanced due to containing an unequal distribution of attacks which affects the

performance of the models. These datasets require preprocessing for further analysis of various machine learning techniques.

Table 1: Description of Available Benchmark Datasets

Sr. No	Name of the dataset	Total number of instances	Type of attack	Number of Features	Availability	Labelled/ Unlabelled
1	KDD-Cup'99 [62-64]	4000000 Imbalanced classes	Normal DoS, Probe, U2R, R2L	41	Freely Available http://archive.ics.uci.edu/ml/datasets/kdd+cup+1999+data	Labelled
2	NSL-KDD [64-65]	Training set= 489431 Test set = 311027	Normal DoS, Probe, U2R, R2L	41	http://www.unb.ca/cic/datasets/nsl.html	Labelled
3	Kyoto 2006+ [65]	Covers three years of real traffic data (2006-2009)	Multiple	24	http://www.takakura.com/Kyoto_data/	Labelled
4	ISCX 2012-Information Security centre for excellence [66]	Training Dataset = 9 Testing Dataset = 9	Normal Attack	9	http://www.unb.ca/cic/datasets/ids.html	Labelled
5	CICIDS2017 [68]	Contains total 5 days data, i.e. Monday to Friday.	Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS	80	http://www.unb.ca/cic/datasets/ids.html	Labelled
6	DEFCON [66]	Contain only attack traffic during DEFCON competition	Port Scan, BufferFlow attacks	No Feature Set available	http://cctf.shmoo.com	Unlabelled
7	DARPA Datasets [67]	Multiple datasets	DoS, Probe, U2R, R2L	Multiple Dataset	http://ll.mit.edu/IST	Labelled
9	UNSW-NB15 [69][73]	Training set = 175,341 Testing Set = 82,332	Fuzzers Analysis, Backdoors, DoS, Exploits, Generic	49	https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys	Labelled

1.4 Anomaly-based ID Techniques

In Anomaly-based ID, techniques can be categorized mainly into three classes: Statistical, Knowledge-based or Machine learning as depicted in Figure 3.

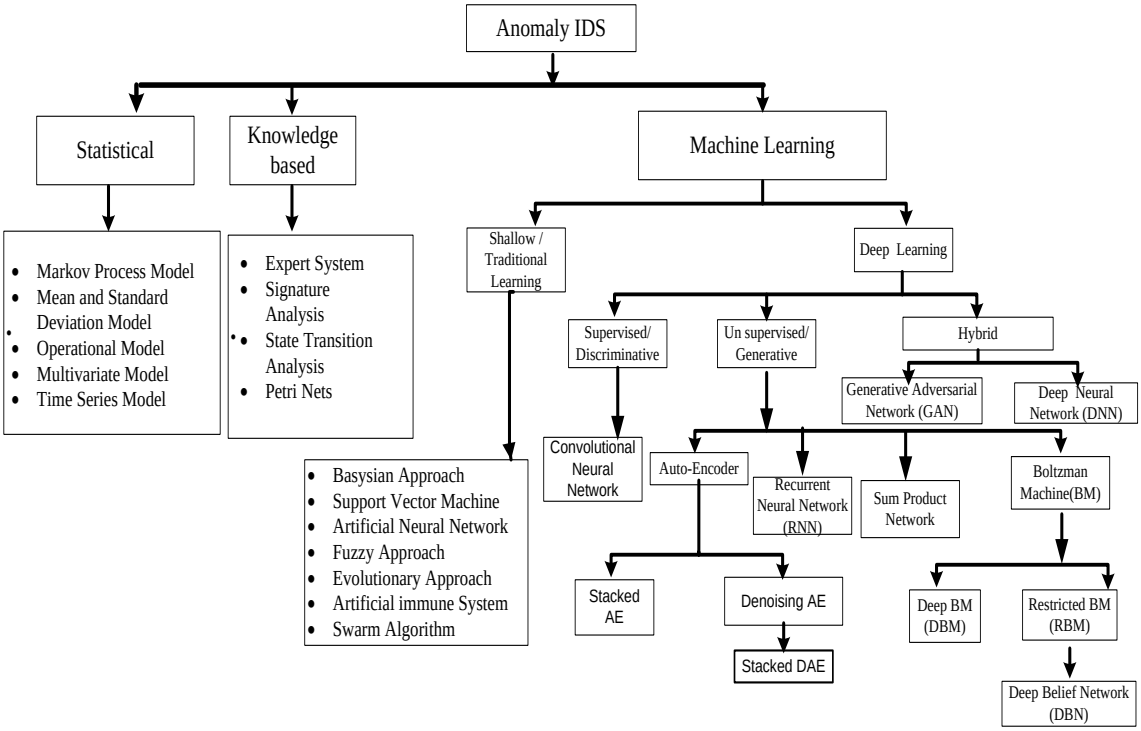

Fig.3 Categorization of Anomaly Techniques

Statistical Techniques:

For Statistical approaches, previous knowledge, as well as frequent signature updates, is not required. It can detect low and slow attacks, especially DoS attacks [31]. Statistical tests are used to check whether the observed behaviour is different from expected behaviour. The limitation of this technique is that the learning process takes a very long time to achieve accuracy and effectiveness and the basic assumption of the quasi-stationary process is not fully met in the real world intrusion detection system.

Knowledge-Based Techniques:

Knowledge-based IDS basically gathers knowledge about specific attacks and system vulnerabilities [31]. Gathered knowledge is used to identify the attacks, and if an event is not identified as an attack, no action is taken. The expert system, Petri Nets, Signature Analysis and State Transition are the various techniques of knowledge-based IDS. The strengths of these techniques are that they are flexible, scalable and robust techniques. The accuracy rate of results produced using these techniques are high with low false alarm rate. For keeping knowledge-based IDS effective, attack data need to be updated regularly which is a very time-consuming process and is the main limitation of knowledge-based IDS.

Machine Learning /Deep Learning Techniques:

Generally, machine learning is a branch of artificial intelligence that learned or adapted to the new environment [55]. It allows the programs to finds and learns the patterns within data. It explores various algorithms also called machine learning algorithms that can learn from and then make predictions on data. The algorithm usually operates based on the features that represent the characteristic of the object. Machine learning techniques are mainly classified into shallow/traditional techniques or deep learning techniques. Bayesian Approach, Fuzzy approach, Evolutionary algorithm, Swarm intelligence, ANN comes under the category of shallow techniques [54]. These techniques work better than statistical and knowledge-based techniques like flexible, high detection rate, generalize the model from limited information and learning by example in the field of intrusion detection [4][55]. However, these techniques suffer from the limitation of manual feature extraction, lower detection accuracy for large and imbalanced datasets, incapable of working efficiently with multidimensional data, requiring background knowledge to determine the number of clusters, high false positive rate etc. [55].

In order to address these limitations, a subset of machine learning techniques called deep learning technique been proposed. Deep learning techniques have advantages of automatic feature extraction, able to handle labelled or unlabeled data with more efficiently. High Processing abilities of GPU over shallow machine learning techniques [57]. These techniques have been successfully employed in the fields of natural language processing, speech recognition, computer vision, audio recognition, machine translation and social network filtering. However, the employment of deep learning techniques in the field of Intrusion detection is still an emerging area [34] [58-60]. In this research work, we focus on the employment of deep learning techniques for detecting the intrusion effectively.

2. Literature Review

A critical literature review of machine learning and deep learning based ID techniques is conducted in the last five years to find out the behaviour of intruders and various malicious activities. In this section, the major findings of the literature review have been described. Although various techniques are available for intrusion detection, still attackers are breaching the security at some level by changing the features of intrusions. Various detection methods have been described in the literature to detect intrusions. On the basis of literature review, challenges and research gaps in the field of network-based intrusion detection system have been found which are discussed in the next section.

Machine learning Techniques has been divided into Shallow Machine learning Techniques and deep learning techniques as described in Section 2.1 and 2.2 respectively.

2.1 Shallow Machine Learning Techniques for Intrusion Detection

In the previous decade, a number of researchers have applied various machine learning techniques in the field of intrusion detection, and studies revealed that the current IDS is unable to handle network traffic due to the change in the features by intruders. The brief literature review of shallow machine learning techniques is given as under:

Tabakhi et al., (2014) [5] presented UFSACO, a multivariate filter method based on ant colony optimization. The method is an iterative improvement process where each feature has an equal chance of being selected in all iterations. The strength of this method is that it effectively reduces dependency between selected features. The limitation of this approach is that it is incapable of eliminating irrelevant features. Tabakhi & Moradi, (2015) [6] proposed unsupervised feature selection methods based on the ACO algorithm to select a high-quality feature subset within a reasonable time. This method outperforms the existing methods, but there is a need to control the randomness in the ACO algorithm.

Belavagi & Muniyal, (2016) [7] designed a NIDS with different supervised machine learning classifiers like Logistic Regression, Support Vector Machine, Gaussian Naive Bayes and Random Forest. For checking the performance of various classifiers, algorithms are tested on NSL-KDD dataset, and it is concluded that Random Forest outperforms other classifiers. It results in lowest FPR and highest TPR in identifying attacks and obtained 99% accuracy. But still, there is a need for classifiers that can be used for multiclass classification.

Ashfaq et al.,(2017) [8] in another research work developed a novel fuzziness based semi-supervised learning(SSL) approach by utilizing unlabeled samples assisted with a supervised learning algorithm to improve the classifier's performance for the IDSs. NSL-KDD dataset was used to evaluate the model, but the limitation was that the performance of the model was studied only the binary classification task. In another research work,Yaseen et al.,(2017) [9] proposed multilevel hybrid intrusion detection model using SVM and EVM to improve the performance of detection accuracy and evaluation was done on KDD 99 dataset. The proposed model showed high efficiency in attack detection with 95.75% accuracy and shorter training time. This technique is better for known attacks, and efficient classifiers are required for novel attacks.

Aljumah, (2017) [10] have used a trained Artificial Neural Network algorithm to detect DDoS attacks (ICMP, UDP, TCP) that will flag malicious and genuine data traffic and will save the network from losing performance. ANN was unable to detect some DDoS attacks because it was trained with old data patterns and thus proving that old datasets or improper training can display poor results. When the ANN is trained with old datasets, the

system responded poorly with 92% of detection accuracy, and when the system is trained with up-to-date datasets, the accuracy was 98%. So accuracy depends upon the dataset. So there is a need for the up-to-date and balanced dataset.

Roshan et al., (2018) [11] proposed an adaptive design of intrusion detection systems based on Extreme Learning Machines. The NSL-KDD dataset is used to evaluate the proposed model, and it is found out that it can detect known and novel attacks with an acceptable rate of detection and false positives.

Ali et al., (2018) [12] proposed a PSO-FLN classifier for the problem of intrusion detection and validated based on the benchmark dataset KDD99. PSO-FLN has outperformed ELM and FLN classifiers in the testing accuracy. But for some classes like R2L, it does not show accurate results because of the limited available amount of training data for such a class.

A summary of the findings of research work on shallow machine learning techniques for intrusion detection from 2014-2018 is given in Table 2.

Table 2: Summary of research work on shallow machine learning techniques

Author(s)/Year/Ref.	**Dataset**	**Method / Technique**	**Advantages/ Results**	**Limitation**
Tabakhi et al., (2014) [5]	Several Standard Datasets such as Wine, Hepatitis etc.	Unsupervised Feature Selection Ant Colony optimization (UFSACO)	Effectively reduce dependency between selected features.	Incapable of eliminating irrelevant features
Tabakhi & Moradi, (2015) [6]	Wine, Dermatology, Sonar, and Arrhythmia datasets	Feature selection method based on Ant colony optimization	Effectively removed irrelevant and redundant features.	New state transition rule can be developed to control the randomness in the ACO algorithm
Belavagi & Muniyal, (2016) [7]	NSL-KDD	Logistic Regression, Gaussian Naive Bayes, Support Vector Machine and Random Forest.	Higher Accuracy, Lowest FPR, Highest TPR (Random Forest Best)	Classifiers required for multiclass classification.
Yaseen et al., (2017) [9]	KDD -99	Multilevel hybrid model using SVM and ELM	High Accuracy, low FAR, Shorter Training Time	Speed up data analysis with the help of multi-agent system characteristics.
Aljumah , (2017) [10]	The mirror image of real-life environment network	Artificial Neural Network	Average accuracy with old datasets. High Accuracy with new datasets.	Unable to handle DDoS attacks that use encrypted packet headers.
Ali, (2018) [12]	KDD-99	Particle swarm optimization-Fast Learning Network	Outperformed ELM and FNN Classifier in the	R2L has obtained less accuracy due to limited samples.

		(PSO-FLN)	testing accuracy.	
Viegas et al.,(2018) [13]	Biological and Textual datasets.	Genetic Programming for Feature Selection and NB algorithm for classification.	Works well both balanced and unbalanced data and capable of selecting a better set of discriminative features	Combination of feature selection with feature construction may be used to Improve the classification performance.

It can be observed from the above-cited research on intrusion detection using shallow machine learning techniques, that these suffer the limitations of manual feature extraction, inefficient to handle raw, unlabeled or high dimensional data, degrades accuracy in case of large dataset, required data labelling which is expensive, time-consuming and tedious task [32].

2.2 Deep learning Techniques

Deep learning Techniques have been used by researchers due to several reasons like it requires fewer efforts for feature engineering, flexible adaptation to novel problems, make it possible to work upon big data. As depicted in Fig 3, these techniques are mainly divided into three classes, namely, Supervised, Unsupervised and Hybrid Techniques [48].

2.2.1 Supervised / Discriminative Deep Learning Techniques

Discriminative Deep learning works on the principal of supervised learning in which the expected result is provided at the time of input [61]. Here the single method is used for feature extraction and classification task. The significant methods used for supervised deep learning methods are described below.

- **Convolutional Neural Network (CNN)**

  These are a special form of feed-forward ANNs which works under supervised learning. These networks are made up of neurons with learnable weights and biases [42]. These models are designed to process data that comes in the form of multiple arrays and eliminates the need for manual feature extraction. It works by withdrawing relevant features directly from images without retaining. Feature identification is the principle application of ConvNets. The automated feature extraction of ConvNets makes it highly accurate for computer tasks [14]. The architecture of CNN is shown in Fig. 4. The limitation of CNN is that it requires a long training time and large data set [42].

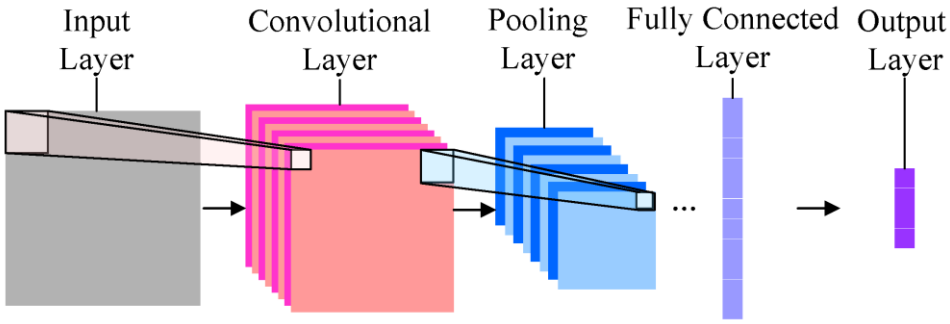

Fig. 4 Architecture of CNN

2.2.2 Unsupervised / Generative Deep Learning

In unsupervised learning, no teacher is provided, that means no training will be given to the machine. Unsupervised learning is the training of machine using information that is neither classified nor labelled and allowing the algorithm to act on that information without guidance. Various deep learning techniques are discussed in this section where deep learning methods are used for feature extraction, and shallow techniques are used for classification tasks.

- **Auto Encoder**

  An autoencoder is trained to attempt to copy its input to its output. Autoencoders are used for dimensionality reduction or feature learning by transforming high dimensional data into a lower dimensional code. Data will be recovered from the code by a decoder network. Initially, random weights are assigned to both encoder and decoder networks and trained by observing the difference between the original data and output obtained from encoding and decoding. Then the error is propagated back through the decoder and encoder network respectively, and this system is known as auto-encoders. The architecture of Auto Encoder is shown in Fig. 5

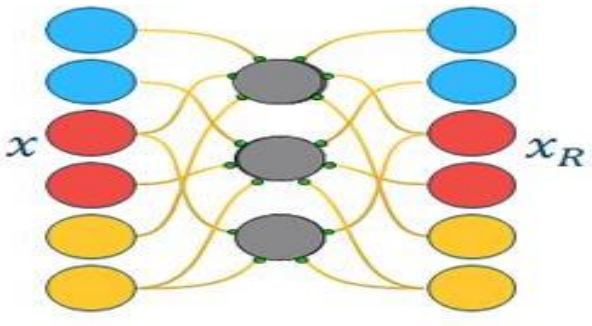

Fig. 5 Architecture of Auto Encoder

- **Recurrent Neural Network (RNN)**

The other deep learning models do not take the time series data into account. Due to this, it is not suitable to learn features for the time series data. RNN is an extension of a conventional feed forward network. It is a sequential learning model and better to use for sequential tasks like speech and language. It learns the features from memory of previous inputs and has cyclic connections, making them powerful for modelling sequences. RNNs have been found to be very good at predicting the next character in the text or the next word in a sequence, but they can also be used for more complex tasks. The best performance is obtained by RNN in many applications such as natural language processing, speech recognition and machine translation. RNN has a disadvantage that it cannot capture long-term dependency. It causes vanishing gradient descent problem. LSTM models are presented to prevent the gradient exploding by learning long term dependency. Memorizing information for long periods of time, each common hidden node was replaced by LSTM cell. The figure of the RNN is depicted in Fig. 6

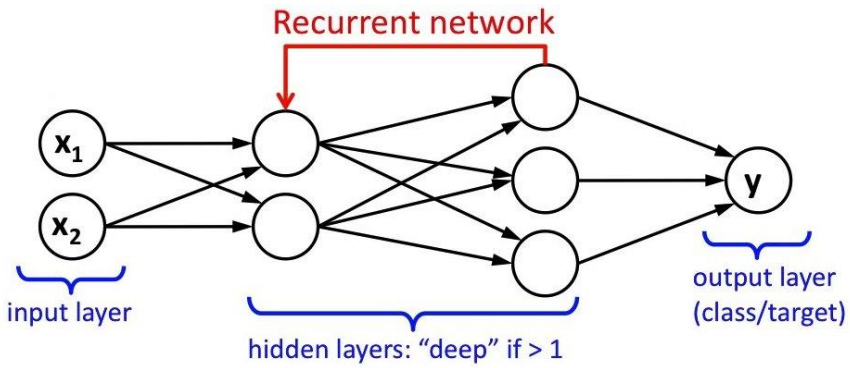

Fig. 6 Architecture of RNN

- **Sum-Product Network (SPN)**

  SPN is a class of deep probabilistic models that consists of many layers of hidden variables and can have unbounded tree width. These models have obtained impressive results in many tasks such as image completion and image classification.

- **Boltzmann Machine (BM)**

  Boltzmann Machines (BM) is the form of log-linear Markov Random Field (MRF), where the energy function is linear in its free parameters. We can introduce hidden nodes to make them powerful enough to represent complicated distribution. By introducing more hidden variables, we can increase the modelling capacity of the Boltzmann Machine. RBM is the most popular version of BM. For regular RBM, the relationships between visible units and hidden units are restricted to be constants that certainly downgrade the representation capability of the RBM. The figure of BM is depicted in Fig 7.

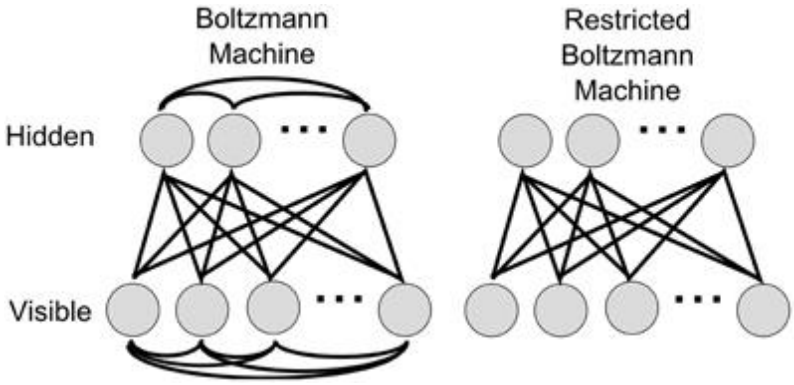

Fig 7. The architecture of Boltzmann Machine

2.3 Deep Learning Techniques based Intrusion Detection

This section describes the significant research work using deep learning techniques for intrusion detection described below.

CNN based intrusion detection: Liu et al., (2018) [15] implemented PL-CNN and PL-RNN techniques for attack detection using CNTC-2017 Webshell dataset, DARPA-98, KDD-99 and CSIC-2010 HTTP dataset. The model contains 1 hidden layer with 128 hidden states. The accuracies achieved are 99.36% and 99.98% using PL-CNN and PL-RNN respectively for subsets of datasets used in their experiments. The authors implemented PL-CNN and PL-RNN as a black box and are not able to explain the results produced by these techniques.

Autoencoder based intrusion detection: Javaid et al., (2016) [16] has used a self-taught deep learning scheme in which unsupervised feature learning has been employed on training data using sparse-auto encoder. Different metrics were used to measure performance. The accuracy of 2-Class was 88.39 %, and the Accuracy of 5 Class was 79.10%. Here, SoftMax classifier was used for feature learning. This work was further extended using SVM [17]. Qatf et al., (2018) [17] also used self-taught leaning by combining SAE and SVM for network intrusion detection. The author used SVM as a strong Classifier instead of Softmax classifier to increase accuracy. The accuracy for the 2-class was 99.423%, and 5 Class was 99.414%. 10% of KDD Cup dataset containing 494,021 samples for training phase and 311029 samples for testing phase was chosen for this purpose.The higher accuracy was achieved only with a subset of a dataset of KDD dataset.

Aminanto & Kim, (2016) [18] proposed the idea to implement different IDS on each TCP/IP layer and used SAE as a Classifier. The accuracy was 99.4% for IDS-T and 99.9% of IDS-All. The limitation of this approach was that the accuracy achieved only for transport layer including only 6 features and network layer, application layer and data link layer are not considered for it. This approach was difficult to implement in a wireless system.

Kolias et al., (2016) [38] specifically detected the intrusion in a wireless system and offered a dataset containing a rich mingle of normal and attack traffic against 802.11 networks that becomes a public dataset for 802.11 networks. Various machine learning algorithms are checked to validate their dataset in a heuristic manner. Among all the classification results, Impersonation Attack detection is the most disappointing result [38]. Aminanto & Kim, (2016) [19] extended the work of [38] and used SAE as a classifier and ANN as a feature selection for optimizing the detection of impersonation attacks only. 35 attributes were selected for ANN learning. The benefit was that it improved the detection (65.18%) of impersonation attack in real network traffic. The limitation was that focus was given only to optimize the impersonation attacks.

Aminanto & Kim, (2017) [20] again used SAE as feature extraction and selection method instead of the classifier and achieved accuracy 94.81% with Precision 86.15%, detection rate 92.18%, FAR 4.40% and F1 89.06%. AWID dataset is used for this purpose. In the SAE network, 2 hidden layers were used containing 100 and 50 neurons accordingly. High false alarm rate still leads to a severe impact on IDS and needs to be reduced in the future.

Aminanto et al., (2018) [21] applied D-FES as a clustering method on AWID dataset and reduced the FAR to 0.012% and achieved detection accuracy equals to 99.918% .The author got the highest accuracy only limited to impersonation attacks.

Muna et al., (2018) [22] used the Deep Auto Encoder to address the issue of FPR and for this NSL-KDD and UNSW-NB15 datasets were chosen.The detection rate and FAR on NSL-KDD was 99% and 1.8% whereas for UNSW-NB15 the detection rate was 93% and FAR was 8.2%.The author got good detection rate and FAR by using one input layer (41 nodes), three hidden layers (10, 3, 10 nodes) and output layer (41 nodes) for the DAE model .The limitation of this model was that it suffered from high computational cost related to training DAE.

LSTM-RNN based intrusion detection: Staudemeyer & Omlin, (2013) [24] applied LSTM-RNN as a classifier and got a satisfactory result. Staudemeyer,(2015) [25] has again applied LSTM-RNN in 2015 and achieved an accuracy of 93.82% with cost 22.13 %, Good accuracy achieved by choosing learning rate of 0.1, and up to 1000 epochs The author used 10% training KDD dataset for this. The limitation of this model was that it was not suitable for low-frequency attacks.

Kim & Kim, (2015) [26] extended this work by constructing one model that was capable of handling all attacks. The author has applied RNN with Hessian-free optimization and got detection Rate equal to 95.37 % and false alarm rate equal to 2.1% by selecting 32

features as an input vector and taking 3100 samples for training and 400 samples for testing. This approach suffers from less classification accuracy of R2L due to insufficient sample size.Darpa dataset is used by the author who is outdated.

Kim et al., (2016) [27] again applied LSTM-RNN using SGD classifier and got detection Rate = 98.88% with FAR = 10.04% and Accuracy = 96.93 % on 10% KDD dataset. The author got the highest efficiency by choosing learning rate 0.01 and hidden layer 80. The limitation of this work was that it suffers from a high false alarm rate than other approaches.

Kim & Kim, (2017) [29] applied a deep learning approach to find the most appropriate optimizer among six optimizers for LSTM RNN. The LSTM RNN model with a Nadam optimizer was a well-organized intrusion detection classifier with 97.54% accuracy rate, 98.95% detection rate, and 9.98% false alarm rate.The parameters selected for this optimizers are $\alpha = 0.002$, $\beta1 = 0.9$, $\beta2 = 0.999$, $= 10^{-8}$, schedule delay = 0.004. KDD dataset was used which is old and suffered from redundancy problem.

Althubiti et al., (2018) [33] applied the LSTM –RNN model with Adam Optimizer on CSIC-2010 HTTP(target to an e-commerce web application) dataset for binary classification problem. Their work reveals the achievement of accuracy = 99.97 % with Recall= 99.5% and Precision=99.5% by choosing 5 features. The parameters selected by the author for the implementation of LSTM-RNN with Adam Optimizer are learning rate=.001, Beta_1=.9, Beta_2=.999, epsilon=1e-08, Decay=0.0.The author also suggested evaluating LSTM Performance with different optimizers. The dataset used by the author is targeted to the e-commerce web application.

- **DNN based intrusion detection:** Tang et al.,(2016) [34] in another research work applied DNN in SDN environment by choosing only six basic features to simplify the process of attack detection and the model had 75.75% accuracy and 86% Area of ROC curve. The author obtained this accuracy by selecting the dimension for input=6, output=2, hidden layers=12,6,3, initiation parameters 10 for the batch size and 100 for the epoch.This method does not take advantage of deep learning models. Accuracy can be further increased by choosing another feature. Wang et al., (2016) [35] used SC-DNN model which was more capable of classifying sparse attack cases and improves detection accuracy in the real security system. The limitation of this model is that weight parameter and thresholds need optimization at each layer and cluster parameters are determined empirically and not through mathematical theory.

- **RBM based intrusion detection:** In another research area, Seo et al.,(2016) [37] recommended that the accuracy of NIDS not only depends upon the performance of classification algorithm but also based upon the management on noises and outliers in the data used for the classification algorithm's learning. For this RBM is applied on KDD-99 and accuracy achieved are 99.4% with a precision of 99.8%

The findings of the review of various deep learning techniques for intrusion detection are summarized in Table 3.

Table 3: Summarized Review of Deep Learning Techniques for NIDS

Study	Dataset	Method used	Advantages	Disadvantages
Liu et al., (2018) [15]	DARPA-98 CNTC-2017 Webshell dataset ,KDD-99 and CSIC-2010 HTTP dataset.	PL-CNN PL-RNN	Higher Accuracy, Effective end to end detection	Implemented PL-CNN and PL-RNN as a black box.
Javaid et al., (2016) [16] (Focus on Feature reduction ability)	NSL-KDD	Self Taught Learning (STL) association with (Sparce autoencoder, Soft-max) Soft max-weak classifier	Good performance for normal and abnormal detection	Implementation of real-time NIDS with more efficient and active feature learning is required.
Qatf et al., (2018)[17]	KDD-99	STL-IDS based on the STL framework by combining SAE and SVM for network intrusion detection SVM-Strong Classifier)	Exhibits good performance for two categories and five category classification.	Training and testing time can be reduced by using GPU.
Aminanto & Kim, (2016) [18] Feature selection	KDD-99	ANN(used for Feature Selection) Stacked Auto Encoder (used for Classifier.)	Lightweight IDS algorithm on each layer, High detection rate	IDS applied only on Transport Layer and Network layer, Application layer and Data Link layer are not discussed, Difficult to implement in Wireless System
Kolias et al.,(2016) [38]	AWID	Soft Computing Algorithms -J48 and Random Forest	High Accuracy and precision for impersonation attacks.	Achieved a low detection rate which is unsatisfactory.
Aminanto & Kim,(2016) [19]	AWID	ANN(used for Feature Selection) Stacked Auto Encoder(used	Improved impersonation attack detection rate.	Limited to impersonation attacks only.

		for Classifier)		
Aminanto & Kim, (2017)[20]	AWID	SAE is used as a Feature Extraction and Selection Method	High Detection Rate, Improved Accuracy	High false alarm rate still leads to a severe impact on IDS and needs to be reduced in the future.
Aminanto et al., (2018)[21]	Aegean Wi-Fi Intrusion Dataset (AWID)	D-FES (Deep Feature extraction and Selection) Used as a Clustering method	High Detection rate , Low False Alarm Rate	Limited to impersonation attacks only.
Muna et al., (2018) [22]	NSL-KDD, UNSW-NB15	Deep-Auto encoder , Deep Feed Forward Neural Network	Easily detect normal and attack behaviours provides an automated process for feature engineering, Higher detection rate, Lower FAR	Not able to deal with a non-numeric and original range of feature values.
Shone et al., (2018) [23]	KDD-99, NSL-KDD	The non-symmetric deep autoencoder (NDAE), RF Classification Algorithm, DL, Stacked NDAEs	High level of accuracy, Precision and Recall	Not perfect for handling zero-day attacks
Staudemeyer & Omlin, (2013) [24]	KDD-99	LSTM-RNN (As a classifier)	Satisfactory results	LSTM may be applied to more recent datasets.
Staudemeyer, (2015) [25]	KDD-99	LSTM-RNN (As a classifier)	Suitable for classifying high-frequency attacks	Not suitable for novel attacks and for low-frequency attacks.
Kim & Kim, (2015)[26]	DARPA	RNN with Hessian-free optimization.	High Detection Rate , low False Alarm Rate (Able to construct one detection model for all attacks.)	Less classification accuracy of R2L due to insufficient samples. (extended by Kim et al., 2016)[27]
Kim et al., (2016)[27]	KDD-99	LSTM-RNN using SGD classifier	High Detection Rate, High accuracy	High false alarm rate than other approaches. (extended by Kim. J. et al. 2017)[29]
Bontemps et al., (2016) [28]	KDD-99	Collective anomaly detection model using LSTM-RNN	100% collective anomaly detection rate with a threshold of 0.52.	High false alarm rate equal to 63 is obtained while achieving 100% collective anomaly detection rate.

Kim & Kim., (2017) [29]	KDD-99	LSTM- RNN model with Nadam optimizer	High Accuracy , High Detection Rate	High False Alarm Rate which still needs to be resolved.
Putchala, (2017)[30]	DARPA/KDD Cup '99	Gated –RNN (Lighter version of LSTM)	High Accuracy, Less FAR	Only Six high-rank features are considered, and work is focused on dealing with IoT devices only where the processing power is low, and the data size is not huge.
Yin et al.,(2017) [32]	NSL-KDD	RNN-IDS used for classification rather than pre-training.	High Detection Rate , Good for binary and multiclass classification	More training time, the training time may be reduced by using GPU acceleration and avoid exploding and vanishing gradients using LSTM-RNN.
Althubiti et al., (2018)[33]	CSIC-2010 HTTP	LSTM-RNN with Adam Optimizer	Efficient binary classifier, high accuracy	Can be applied on more recent datasets
Tang et Al.,(2016) [34]	NSL-KDD	DNN in SDN Environment (choose sub-feature set) Only Six basic features are used.	Higher Accuracy Rate, Lower False Positive Rate	Accuracy can be further enhanced by choosing another feature.
Wang et al.,(2016) [35]	KDD-99 NSL-KDD	(SC-DNN), spectral clustering, deep neural network	Suitable in complex networks, Improves detection accuracy in a real security system, more capable of classifying sparse attacks cases.	Cluster parameters were determined empirically and not through mathematical theory.
Potluri & Diedrich, (2017) [36]	NSL-KDD	DNN	Better and robust feature extraction.	Parallelization of the DNN training will reduce the computation time.
Seo et al., (2016)[37]	KDD 99	Restricted Boltzmann Machine	High Accuracy and Precision , improved classification performance	Further improvements can be made with combinations of PCA or LDA and RBM.
Zhang & Chen, (2017) [39]	KDD99	RBM-SVM RBM-DBN	Spends less time in training model, suitable for large data intrusion detection	High accuracy achieved on particular dataset but differs when used on other datasets.
Zhang et al., (2017)[40]	NSL-KDD	DBN (Strong Feature extraction and classification ability)	Better classifer, improvement in the speed of intrusion detection.	Can be combined with other models to improve further.

3. Research Issues / Gaps

It is observed from the findings of the above-cited researches for intrusion detection that effective intrusion detection has many issues. The major issues are summarized below.

1. The standard benchmark datasets used by most researchers are large in size, imbalanced and available in a format that is not compatible with deep learning techniques directly. The huge size of the dataset has increased the computational overhead, leading to a delay in detecting the intrusions. Getting the right data in the appropriate format is also a challenge for deep learning projects. Balancing dataset and its pre-processing are the main issue for employment of deep learning techniques for effective intrusion detection [72][73][74][75][31][23].
2. Most of the existing techniques are dependent upon labelled data for training their models, so they are unable to handle zero-day attacks [23][72].
3. Automatic feature learning is a difficult task. With the evolving attack scenarios, features identified to detect one category of attacks may not be suitable for the others. Thus, there is a need to propose a framework which can automatically learn features, reduce the computational time and increase the accuracy [16] [71] [6][31].
4. Some of the intrusions occurred in the organizations might not be reported due to privacy and confidentiality policy of the users. So, it becomes difficult to detect attacks whose signatures are not available [16][76].
5. Generalization is a key challenge in deep learning systems. It is not possible to give a labelled sample of every problem [31].
6. To monitor the network traffic from multiple attacks without degrading performance [32].
7. Presently, high false alarm rate and low detection rate have been considered as critical issues for many types of research in the recent past [11] [27][28][70][75][77].
8. There is a need to develop deep learning models for training data with noise [31].
9. Most research conducted in the field of intrusion detection was validated using smaller subsets of obsolete datasets, that may not be representing network traffic in real-world networks [15][26][27][29].
10. Most research in the field of deep learning is limited to supervised learning that requires large amount of quality labeled data. The performance of these supervised methods relies on the quality and quantity of labelled training data. The availing quality labeled data is a challenging task for network-based intrusion detection. However, unsupervised learning using deep learning techniques is a promising direction for detecting intrusions from un-labeled data.

11. In case of limited availability of labeled dataset, the use of data augmentation using deep learning techniques for improving the detection accuracy is still needs to explore.

4. Problem Formulation

With the growth of Internet facility, the online data is increasing day by day which needs to be secure from intruders. Intruders attack data from multiple locations which are sometimes not traceable. The traditional techniques can detect the known attacks, but unable to detect unknown attacks which motivate the researchers towards machine learning techniques by taking their advantages over the traditional techniques consideration. In the literature, many researchers used machine learning techniques for detecting intrusions. Still, there is some possibility to improve the detection rate and false alarm rate.

The traditional machine learning techniques have certain limitations like manual feature extraction, requires a vast quantity of training data for operation and poor detection results which become a challenge in the heterogeneous environment. To overcome these problems, deep learning, a branch of machine learning, has attracted the researchers due to its several advantages over traditional machine learning techniques. In the literature, deep leaning mostly deployed for natural language processing, speech recognition, computer vision, audio recognition, machine translation, and social network filtering. The literature on deep learning shows that still there is lots of scope in the field of intrusion detection using deep learning techniques. Thus, the deep learning techniques are need of the hour to extract automatic features and improve detection accuracy in terms of detection rate and false positive rate using benchmark intrusion detection datasets.

Therefore, the development of a deep learning based approach for network-based intrusion detection system, that is adaptable, capable of fast learning and presenting classification trade-offs for accurate identification of intrusions is the need of the hour.

5. Research Objectives

The purpose of this proposed research work is to develop a deep learning based approach to detect network intrusions with a low false alarm rate and high detection rate. The proposed approach aims to extract automatic features and improve detection accuracy in terms of detection rate and false positive rate using benchmark intrusion detection datasets. The main objectives of this proposed work are described below.

1. To perform a comparative analysis of conventional / shallow machine learning techniques to identify their problems in detecting intrusions using benchmark datasets.
2. To pre-process the network audit data for analysis of deep learning methods to detect network intrusions.

3. To propose a feature extraction approach for accurate intrusion detection.
4. To propose a deep learning approach, capable of learning to detect network intrusions without supervision, and detects intrusions accurately.
5. To validate the proposed approaches using benchmark datasets for network intrusion detection.

6. Expected Contributions

The proposed work is expected to contribute to detecting the intrusion quickly and accurately by proposing the followings.

- Empirical investigation of machine learning methods for Network based intrusion detection.
- Dimension reduction of network audit data for accurate intrusion detection.
- Deep learning model for accurate detection of intrusion.

7. Methodology

In order to meet the objectives, this work follows the research methodology as depicted in Fig. 8.

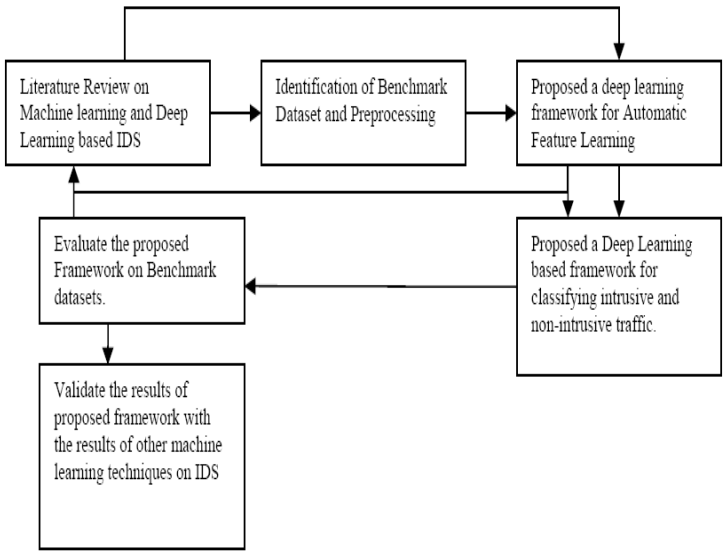
Literature Review on Machine learning and Deep Learning based IDS
Identification of Benchmark Dataset and Preprocessing
Proposed a deep learning framework for Automatic Feature Learning
Evaluate the proposed Framework on Benchmark datasets.
Proposed a Deep Learning based framework for classifying intrusive and non-intrusive traffic.
Validate the results of proposed framework with the results of other machine learning techniques on IDS

Fig. 8 The Proposed Methodology

8. Place of Work

- Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab (India)
- Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab (India)

9. Resources (Hardware/Software/) Required

- Python
- Tensor Flow
- GPU based computer system

Proposed Work Plan

Schedule of proposed work	Time Period					
	Jan 2018 to Jun 2018	July 2018 to Dec 2018	Jan 2019 to Jun 2019	July 2019 to Dec 2019	Jan 2020 to Jun 2020	July 2020 to June 2021
-Literature review						
-Literature review -Proposal Preparation						
-Literature Review -Comparative analysis of conventional / shallow machine learning techniques to identify their problems in detecting intrusions using benchmark datasets.						
-Literature Review -Pre-process the network audit data for analysis of deep learning techniques to detect the network intrusions.						
-Literature review - Propose a deep learning approach for automatic feature learning to reduce the network audit data with the aim of detecting intrusions quickly and accurately from benchmark datasets.						
-Literature Review -To propose a deep learning based approach for detecting the network intrusions with improved detection results in comparison to the existing						
- Validate the proposed approaches using benchmark datasets for network intrusion detection.						
Paper Writing						
-Report Writing						

Fig 9. Timeline activities of the proposed work

Bibliography

1. Lee, B., Amaresh, S., Green, C., & Engels, D. (2018). Comparative Study of Deep Learning Models for Network Intrusion Detection. *SMU Data Science Review*, *1*(1), 8.
2. Symantec, Online available: https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html. Last accessed on 12-02-2019.
3. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2018). A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets. *arXiv preprint arXiv:1806.03517*.
4. Jain, A., Verma, B., & Rana, J. L. (2014). Anomaly Intrusion Detection Techniques: A Brief Review. *Interl. Journal of Scientific & Engineering Research*, *5*(7), 1372-1383.
5. Tabakhi, S., Moradi, P., & Akhlaghian, F. (2014). An unsupervised feature selection algorithm based on ant colony optimization. *Engineering Applications of Artificial Intelligence*, *32*, 112-123.
6. Tabakhi, S., & Moradi, P. (2015). Relevance–redundancy feature selection based on ant colony optimization. *Pattern recognition*, *48*(9), 2798-2811.
7. Belavagi, M. C., & Muniyal, B. (2016). Performance evaluation of supervised machine learning algorithms for intrusion detection. *Procedia Computer Science*, *89*, 117-123.
8. Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484-497.
9. Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. *Expert Systems with Applications*, *67*, 296-303.
10. Aljumah, A. (2017). Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(8).
11. Roshan, S., Miche, Y., Akusok, A., & Lendasse, A. (2018). Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines. *Journal of the Franklin Institute*, *355*(4), 1752-1779.
12. Ali, M. H., Al Mohammed, B. A. D., Ismail, A., & Zolkipli, M. F. (2018). A new intrusion detection system based on Fast Learning Network and Particle swarm optimization. *IEEE Access*, *6*, 20255-20261.
13. Viegas, F., Rocha, L., Gonçalves, M., Mourão, F., Sá, G., Salles, T., ... & Sandin, I. (2018). A genetic programming approach for feature selection in highly dimensional skewed data. *Neurocomputing*, *273*, 554-569.
14. Tirumala, S. S. (2014). Implementation of evolutionary algorithms for deep architectures. CEUR Workshop Proceedings.
15. Liu, H., Lang, B., Liu, M., & Yan, H. (2018). CNN and RNN based payload classification methods for attack detection. *Knowledge-Based Systems*.
16. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016, May). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
17. Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access*, *6*, 52843-52856.
18. Aminanto, M. E., & Kim, K. (2016). Deep learning-based feature selection for intrusion detection system in transport layer.

19. Aminanto, M. E., & Kim, K. (2016, August). Detecting impersonation attack in WiFi networks using deep learning approach. In *International Workshop on Information Security Applications* (pp. 136-147). Springer, Cham.
20. Aminanto, M. E., & Kim, K. (2017, August). Improving detection of Wi-Fi impersonation by fully unsupervised deep learning. In *International Workshop on Information Security Applications* (pp. 212-223). Springer, Cham.
21. Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., & Kim, K. (2018). Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Transactions on Information Forensics and Security*, *13*(3), 621-636.
22. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of Information Security and Applications*, *41*, 1-11.
23. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41-50.
24. Staudemeyer, R. C., & Omlin, C. W. (2013, October). Evaluating performance of long short-term memory recurrent neural networks on intrusion detection data. In *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference* (pp. 218-224). ACM.
25. Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. *South African Computer Journal*, *56*(1), 136-154.
26. Kim, J., & Kim, H. (2015, August). Applying recurrent neural network to intrusion detection with hessian free optimization. In *International Workshop on Information Security Applications*(pp. 357-369). Springer, Cham.
27. Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016, February). Long short term memory recurrent neural network classifier for intrusion detection. In *Platform Technology and Service (PlatCon), 2016 International Conference on* (pp. 1-5). IEEE.
28. Bontemps, L., McDermott, J., & Le-Khac, N. A. (2016, November). Collective anomaly detection based on long short-term memory recurrent neural networks. In *International Conference on Future Data and Security Engineering* (pp. 141-152). Springer, Cham.
29. Kim, J., & Kim, H. (2017, February). An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization. In *Platform Technology and Service (PlatCon), 2017 International Conference on* (pp. 1-6). IEEE.
30. Putchala, M. K. (2017). *Deep Learning Approach for Intrusion Detection System (IDS) in the Internet of Things (IoT) Network using Gated Recurrent Neural Networks (GRU)* (Doctoral dissertation, Wright State University).
31. Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. *Neurocomputing*, *237*, 350-361.
32. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954-21961.
33. Althubiti, S., Nick, W., Mason, J., Yuan, X., & Esterline, A. (2018, April). Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection. In *SoutheastCon 2018*(pp. 1-5). IEEE.
34. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016, October). Deep learning approach for network intrusion detection in software defined networking. In *Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on* (pp. 258-263). IEEE.
35. Ma, T., Wang, F., Cheng, J., Yu, Y., & Chen, X. (2016). A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. *Sensors*, *16*(10), 1701.

36. Potluri, S., & Diedrich, C. (2017). Deep feature extraction for multi-class intrusion detection in industrial control systems. *Int. J. Comput. Theory Eng*, *9*(5), 374-379.
37. Seo, S., Park, S., & Kim, J. (2016, December). Improvement of Network Intrusion Detection Accuracy by Using Restricted Boltzmann Machine. In *Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference on* (pp. 413-417). IEEE.
38. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, *18*(1), 184-208.
39. Zhang, X., & Chen, J. (2017, May). Deep learning based intelligent intrusion detection. In *Communication Software and Networks (ICCSN), 2017 IEEE 9th International Conference on* (pp. 1133-1137). IEEE.
40. Qu, F., Zhang, J., Shao, Z., & Qi, S. (2017, December). An Intrusion Detection Model Based on Deep Belief Network. In *Proceedings of the 2017 VI International Conference on Network, Communication and Computing* (pp. 97-101). ACM.
41. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954-21961.
42. Kumar, V., & Garg, M. L. (2017, November). Deep learning in predictive analytics: A survey. In *Emerging Trends in Computing and Communication Technologies (ICETCCT), International Conference on* (pp. 1-6). IEEE.
43. Omer, K. A. A., & Awn, F. A. (2015). Performance Evaluation of Intrusion Detection Systems using ANN. *Egyptian Computer Science Journal*, *39*(4).
44. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761-768.
45. Van, N. T., Thinh, T. N., & Sach, L. T. (2017, July). An anomaly-based network intrusion detection system using deep learning. In *System Science and Engineering (ICSSE), 2017 International Conference on* (pp. 210-214). IEEE.
46. Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. *Expert Systems with Applications*, *42*(1), 193-202.
47. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. *arXiv preprint arXiv:1701.02145*.
48. Aminanto, E., & Kim, K. (2016). Deep learning in intrusion detection system: An overview. In *2016 International Research Conference on Engineering and Technology (2016 IRCET)*. Higher Education Forum.
49. Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. *Artificial Intelligence Review*, *34*(4), 369-387.
50. Guo, Y., Liu, Y., Oerlemans, A., Lao, S., Wu, S., & Lew, M. S. (2016). Deep learning for visual understanding: A review. *Neurocomputing*, *187*, 27-48.
51. Sarmah, A. (2001). Intrusion detection systems: Definition, need and challenges.
52. Zhang, Q., Yang, L. T., Chen, Z., & Li, P. (2018). A survey on deep learning for big data. *Information Fusion*, *42*, 146-157.
53. Khan, J. A., & Jain, N. (2016). A survey on intrusion detection systems and classification techniques. *Int. J. Sci. Res. Sci., Eng. Technol.*, *2*(5), 202-208.
54. Sheikhan, M., Jadidi, Z., & Farrokhi, A. (2012). Intrusion detection using reduced-size RNN based on feature grouping. *Neural Computing and Applications*, *21*(6), 1185-1190.

55. Umer, M. F., Sher, M., & Bi, Y. (2017). Flow-based intrusion detection: Techniques and challenges. *Computers & Security*, *70*, 238-254.
56. Manzoor, I., & Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. *Expert Systems with Applications*, *88*, 249-257.
57. Chen, X. W., & Lin, X. (2014). Big data deep learning: challenges and perspectives. *IEEE access*, *2*, 514-525.
58. Ponkarthika, M., & Saraswathy, V. R. Network Intrusion Detection Using Deep Neural Networks.
59. Bodström, T., & Hämäläinen, T. (2018). State of the art literature review on network anomaly detection with deep learning. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* (pp. 64-76). Springer, Cham.
60. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. *arXiv preprint arXiv:1701.02145*.
61. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2017). A survey of deep learning-based network anomaly detection. *Cluster Computing*, 1-13.
62. Tabatabaefar, M., Miriestahbanati, M., & Grégoire, J. C. (2017, April). Network intrusion detection through artificial immune system. In *2017 Annual IEEE International Systems Conference (SysCon)* (pp. 1-6). IEEE.
63. Hooks, D., Yuan, X., Roy, K., Esterline, A., & Hernandez, J. (2018, March). Applying Artificial Immune System for Intrusion Detection. In *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)* (pp. 287-292). IEEE.
64. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1-6). IEEE.
65. Protić, D. D. (2018). Review of KDD Cup'99, NSL-KDD and Kyoto 2006+ datasets. *Vojnotehnički glasnik*, *66*(3), 580-596.
66. Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *computers & security*, *31*(3), 357-374.
67. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, *6*, 1792-1806.
68. Jazi, H. H., Gonzalez, H., Stakhanova, N., & Ghorbani, A. A. (2017). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Computer Networks*, *121*, 25-36.
69. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*, *25*(1-3), 18-31.
70. Law, K. H. (2004, August). IDS false alarm filtering using KNN classifier. In *International Workshop on Information Security Applications* (pp. 114-121). Springer, Berlin, Heidelberg.
71. Ghimatgar, H., Kazemi, K., Helfroush, M. S., & Aarabi, A. (2018). An improved feature selection algorithm based on graph clustering and ant colony optimization. *Knowledge-Based Systems*, *159*, 270-285.
72. Kim, K., & Aminanto, M. E. (2017, September). Deep learning in intrusion detection perspective: Overview and further challenges. In *2017 International Workshop on Big Data and Information Security (IWBIS)* (pp. 5-10). IEEE.

73. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1-6). IEEE.
74. Kabir, E., Hu, J., Wang, H., & Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems*, *79*, 303-318.
75. Cieslak, D. A., Chawla, N. V., & Striegel, A. (2006, May). Combating imbalance in network intrusion datasets. In *GrC*(pp. 732-737).
76. Fiore, U., Palmieri, F., Castiglione, A., & De Santis, A. (2013). Network anomaly detection with the restricted Boltzmann machine. *Neurocomputing*, *122*, 13-23.
77. Yu, Y., Long, J., & Cai, Z. (2017, October). Session-based network intrusion detection using a deep learning architecture. In *International Conference on Modeling Decisions for Artificial Intelligence* (pp. 144-155). Springer, Cham.